DEALER.COM

White Ops

Protecting Your Digital Advertising Investment

New approaches and partnerships to combat fraud and maximize ROI.

DEALER.COM

Table of Contents

Abstract

If you're employing digital advertising in your marketing strategy, you know what a powerful tool it can be and how it makes it easy to track your return on investment. But the rising threat of advertising fraud makes the protection of your investment increasingly important.

It's more essential than ever to understand the risks of ad fraud and stay one step ahead of fraudulent practices. Discover the human and automated threats to the automotive advertising ecosystem and learn what Dealer.com is doing to protect dealerships.

Section 1

The Rising Importance of Security in Digital Advertising

The rapid evolution of today's digital marketing and retailing technologies are transforming the automotive industry. Through both SEO and paid digital advertising you have the power to reach a greater number of potential customers. According to the 2018 Car Buyer Journey Study by Cox Automotive, car buyers who choose to shop online spend 60% of their time on digital channels.

As the online auto market grows in importance, so does the need to safeguard your investment against those with less-than-honorable intentions — particularly as it relates to digital advertising fraud. In this paper we'll examine the vulnerabilities that exist within the digital space, the risk to the automotive industry, and the steps Dealer.com is taking to help protect the return on investment of your digital marketing efforts.

We will explore:

- How and why digital advertising is vulnerable to fraud,
- The bottom-line impact of fraudulent activities,
- Emerging challenges and opportunities in fraud prevention today,
- Dealer.com's approach to fraud prevention.

Section 2

Where There's Money, There's Fraud

Global digital ad spend is predicted to total $273 billion by the end of 2018, accounting for 43.5% of all advertising spend. This would represent 17.7% growth from last year, demonstrating that the digital ad market is truly thriving.[1]

Unfortunately, this amount of money tends to attract people with less-than-pure intentions. Cybercriminals have realized that there's a significant amount of money to be made by siphoning off ad revenue. And so, investments in ad fraud have increased.

What we call "ad fraud" is actually comprised of three issues: ad viewability, brand safety, and bot fraud. Unscrupulous publishers or cybercriminals can exploit any one of these areas to profit off of advertising spend.

$273B

Global digital ad spend is expected by the end of 2018.

1 eMarketer, "Global Ad Spending Forecast for 2018," May 2018

Ad viewability

Viewability is just what it sounds like — how viewable an ad is on a webpage. Issues with viewability generally occur when an ad is purposely or mistakenly placed somewhere where it won't garner many views, such as "below the fold" of a webpage. In extreme cases, ads are sent to inventory units underneath other ads, making them totally invisible to the users an advertiser has paid for (and therefore fraudulent).

Brand safety

When it comes to digital marketing, brand safety is the effort to ensure that ad placement aligns with a brand's reputation and goals. A placement may not be brand-safe if it's next to violent or graphic content, but brand safety can also be affected if an ad shows up next to irrelevant content. For example, an ad for a used car dealership in Tallahassee doesn't make much sense on a site for local news in Detroit. Again, unsafe placements can be made purposely — which is fraud — or unintentionally.

Bot fraud

Bot fraud is deliberately attempting to inflate views or clicks to ads by having bots visit ads or pages to generate fake traffic. Since it looks like the ads were served to humans, the perpetrator still gets paid. To make things worse, the traffic is often sold at an artificially low price. Of course, none of these "customers" will ever make a purchase, leading to wasted advertising spend and lost revenue for publishers. According to Hewlett Packard, bot fraud provides criminals with the best payout potential with the lowest effort and risk.

Without intervention, ad fraud is only expected to grow as cybercriminals become more and more sophisticated. But, as we'll explain in the next section, bot fraud presents the greatest threat.

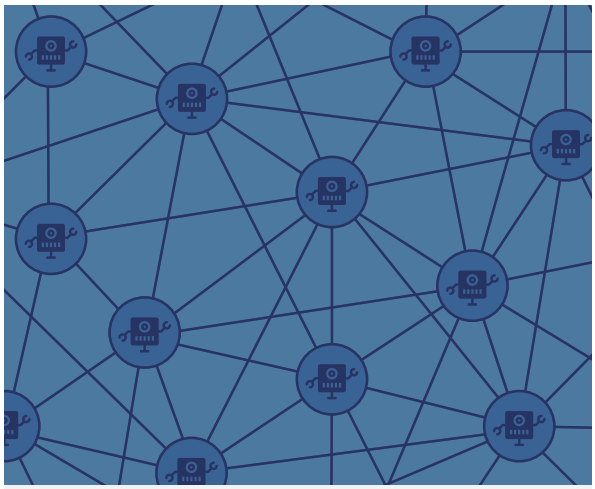
How Bots Conduct Ad Fraud

Though there are some threats that humans can execute alone, the majority of today's ad fraud is perpetrated by vast networks of automated bots. Unlike human-perpetrated fraud, which requires a certain level of skill and investment, bot fraud is inexpensive and ubiquitous. According to the Association of National Advertisers (ANA), advertisers around the world lose an estimated $6.5 billion each year due to bot fraud. 9% of all display spending—and a whopping 22% of video ad spending—is lost to fraudulent activity.[2]

Early bots lived on massive data servers and behaved mechanically, making them easy to catch. But today's bots lie hidden on residential computers, installed when an unwitting user visits the wrong website or downloads a malicious file. Over 75% of the fraud observed in last year's ANA (Association of National Advertisers) Bot Baseline came from computers with mixed bot and human usage, indicating that this kind of fraud is quite widespread.[2]

One bot on its own doesn't pose much of a threat, but vast networks of bots—known as "botnets"—work together by the hundreds of thousands to perpetrate fraud.

Even more concerning, bots can use the data on their host computers to masquerade themselves as human users. To the naked eye, bot behavior is nearly indistinguishable from human behavior.



$6.5B

Lost to advertising bot fraud each year.

2 http://www.ana.net/content/show/id/botfraud-2017

Section 3 - Continued

Though bots can perpetrate ad fraud in a number of ways, the most pressing one for advertisers is paid traffic acquisition, otherwise known as traffic sourcing. In fact, purchased traffic contains 3.6 times more fraud than non-purchased traffic.[2]

Buying traffic is a widely accepted practice, but publishers don't always have the tools to determine if the traffic vendor they're working with is legitimate. Without a discerning eye or bot detection software, a publisher has no idea whether they're purchasing legitimate views and clicks—or a host of bots.

Sometimes, unscrupulous publishers intentionally seek out bot traffic—or even build "cash-out" sites that only exist to generate ad revenue. These sites—which have no real content nor human visitors—make up roughly 20% of all the domains on the internet. However, the vast majority of publishers are victims of ad fraud rather than perpetrators; as the market for inexpensive traffic grows, they lose money too.[2]

As you can imagine, traffic sourcing fraud leads to trust issues between advertisers and publishers. When publishers can't be sure that the traffic they're offering is real, advertisers may spend a hefty chunk of their marketing budget on clicks that won't turn into conversions. Conversely, advertisers may be hesitant to invest those marketing dollars, missing opportunities to reach their target audiences.

2 http://www.ana.net/content/show/id/botfraud-2017

Section 4

Challenges of Fraud Prevention

Given ad fraud's prevalence and potential costs—not to mention dealers' increasing reliance on digital advertising—the stakes are pretty high when it comes to fighting fraud. And with the perpetrators of fraud continually adapting their techniques, constant vigilance is essential.

However, fraud prevention can be hindered by the fact that bots and botnets are constantly changing. Cybercriminals alter their algorithms almost daily to evade detection and improve their camouflage as human users. As a result, they've engaged governments and private cybersecurity organizations in an arms race, where each party works to outsmart the other.

Finally, it's hard to pinpoint who exactly is responsible for fraud prevention. Sell-side platforms selling advertising inventory? Demand-side platforms managing ad placement? Individual publishers? It remains an ongoing debate.

At Dealer.com, we believe every piece of the digital advertising ecosystem is responsible for creating a safe environment that leverages advertising fraud detection and prevention technologies. We also believe that you're not powerless in the fight to protect yourself against fraud.

Section 5

How Dealer.com Is Combating Advertising Fraud

At Dealer.com, we take advertising fraud seriously and have made it our mission to help protect the investments our clients make in advertising providing a clear, transparent view of how advertising dollars are impacting sales. Our commitment to help protect our customers against fraud can be summarized in two words — partnership and proactivity.

Strong partnerships

To help combat fraud, Dealer.com has partnered with three industry leaders — White Ops, The Trustworthy Accountability Group (TAG), and MOAT Analytics.

White Ops is a cybersecurity company that protects businesses from automated online threats like ad fraud, account takeovers, and fake engagement conducted by malicious bots. Even if a bot perfectly impersonates human behaviors, White Ops' Human Verification technology is able to detect it. This capability, combined with a unique "white hat" perspective on the cybercriminal mindset, has helped White Ops become a trusted partner to brands like Adobe, The Trade Desk, and AppNexus. 100% of all impressions on the Dealer.com advertising platform are reviewed by White Ops.

The Trustworthy Accountability Group (TAG) is the leading global certification program focused on fighting criminal activity and increasing trust in digital advertising by working to eliminate fraudulent traffic, combat malware, prevent Internet piracy, and promote greater transparency.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

MOAT Analytics is a true cross-platform analytic solution provider. They measure advanced ad engagement metrics to provide full transparency into how ad viewers engage with the content in an ad. MOAT has a proprietary, in-depth methodology for detecting invalid traffic. The thousands of hours they have invested in blocking non-human traffic have allowed them to detect and help block it.

Dealer.com is the first and only automotive-specific digital advertising provider to partner with White Ops and receive the Certified Against Fraud seal by the Trustworthy Accountability Group — both in connection with the steps taken to prevent advertising fraud. Dealer.com has also partnered with MOAT to bring more transparency to your advertising analytics.

A proactive approach

Working proactively with partner organizations, Dealer.com's proprietary Demand Side Platform (DSP) utilizes White Ops' sophisticated filtering mechanisms, in combination with advanced machine learning and real-time bidding technologies, to determine whether the entity behind an "impression" is a real human. All of this is done in milliseconds, ensuring opportunities are both carefully reviewed and quickly acted upon. In fact, over a period of just six months we have proactively blocked almost 700 million bots from our platform, preventing more than $1.75 million from potentially falling victim to ad fraud.[3]

Dealer.com also engages in an intensive review process. Aided by our partnerships with White Ops and TAG, we carefully vet all the domains where we're buying ad inventory and blacklist any that appear to be malicious in nature.

This combination of partnership and proactivity allows Dealer.com to effectively block advertising fraud, helping it become the first automotive-specific digital advertising company to carry the coveted TAG Certified Against Fraud seal.

> "Dealer.com is tackling this important issue head-on, and we commend their leadership in fighting advertising fraud in the automotive industry. We are excited to welcome Dealer.com as one of the recipients of the TAG Certified Against Fraud Seal, and we look forward to continuing to work with them to promote brand safety by eliminating fraudulent digital advertising."
>
> **Mike Zaneis, CEO of TAG**

3 Dealer.com Internal Data, January–June 2018

Maintaining Vigilance Is Key

Make no mistake—while digital advertising is the most effective way to reach potential car buyers, it's not without its vulnerabilities. In order to protect your investment, and fully leverage the power of the medium—it takes vigilance and a partnership with someone looking out for your best interests.

There's no way to completely eliminate the threat of digital advertising fraud, particularly since the perpetrators continually evolve their methods, but there are ways to effectively manage the threat. Dealer.com understands that a digital ad is only as effective as the technology deployed to ensure its integrity. As a client, it's important to work with someone who's just as focused on protecting your investment as you are.

References

Hewlett Packard Study

http://static.politico.com/b9/55/4e3ce4c
c41d88401e264dcacc35c/hpe-security-
research-business-of-hacking-may-2016.pdf

ANA 2016 Study

https://cdn2.hubspot.net/hubfs/3400937/
White%20Papers/ANA_WO_BotBaseline
2016-2017.pdf?t=1535578757792

eMarketer Global Ad Spending Forecast for 2018

https://www.emarketer.com/content/
global-ad-spending